

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR LETTERS PATENT

**Authentication Methods and Systems for Accessing
Networks, Authentication Methods and Systems for
Accessing the Internet**

Inventor(s):

Paramvir Bahl
Srinivasan Venkatachary
Anand Balachandran

ATTORNEY'S DOCKET NO. MS1-493US

1 **TECHNICAL FIELD**

2 The present invention relates to authentication methods and systems for
3 accessing networks. In particular, the invention relates to authentication methods
4 and systems for accessing the Internet.

5

6 **BACKGROUND**

7 As network technologies continue to evolve, the possibility of connecting
8 people and organizations together in more efficient arrangements grows.
9 Networks such as the cellular phone networks give individuals the ability to move
10 around freely, yet still communicate over the telephone with other individuals. For
11 example, in the last few years the explosive growth of the use of cellular phones
12 has increased tremendously the ability of people to connect with other people from
13 a variety of different locations (i.e. in the car, at a restaurant, in the super market).
14 As societies become more and more mobile, new solutions are required to satisfy
15 the growing demands and needs of these mobile individuals.

16 As one example, consider the traditional network paradigm for Internet
17 access. Traditionally, there are a couple of different ways for an individual to
18 access the Internet. First, the individual might have a personal account with an
19 Internet Service Provider (ISP) whereby they can access the Internet through, for
20 example, their home computer. Their home computer establishes a link with the
21 ISP through a modem or special communication line. Once the link is established,
22 generally over a wired line, they can typically use ISP-provided software to
23 browse the Internet. In this example, an individual's Internet access is either tied
24 to their wired link provider, or to the ISP through which they have their account.
25 Second, an individual might be able to access the Internet through a network that

1 is provided and maintained by their employer. While they are at work, they can
2 access the Internet through the use of employer-provided resources. In this
3 example, an individual's Internet access is tied to their employer and/or their
4 employer's resources.

5 Neither of these paradigms provides an individual with the freedom to
6 access the Internet from any location and without any dependence on a particular
7 ISP or their company. Rather, Internet accessibility for these individuals is
8 necessarily tied to either or both of (1) signing up for an account with a particular
9 ISP for Internet access, or (2) being a member of a particular corporation through
10 which Internet access is provided. It would be desirable to eliminate the
11 dependence of Internet access on either or both of these elements.

12 Presently, there is much enthusiasm around the impending deployment and
13 availability of the so-called "third generation" (3G) wide-area cellular networks.
14 These 3G wide-area cellular networks will give individuals the ability to connect
15 to other individuals, via a cellular phone, from many different locations.
16 Furthermore, these networks will enable individuals to transmit and receive data
17 packets which are necessary for Internet communications.

18 There are, however, limitations that are inherent with both the current wide-
19 area cellular networks and the future 3G wide-area cellular networks that make
20 their use as an Internet connectivity medium less than desirable. For example,
21 current wide-area data networks (e.g. which use a Ricochet modem from
22 Metricom) support transmission rates that are about 50 Kbps. In the next few
23 years, when 3G wide-area cellular networks are available, the data packet
24 transmission rates are expected to go up to around 2 Mbps per cell size. Each cell
25 is generally sized between 1 to 2 miles in diameter, depending on where the cell is

located. A data rate of 2 Mbps per cell size means that the maximum data rate an individual in a cell can hope to get will be around 2 Mbps when there are no other individuals using the network. A more realistic scenario is the case where there are several hundred individuals in a single cell. In this case, any individual might get only 100 to 150 kbps of bandwidth for data transmission. This transmission rate is frustratingly slow and will inevitably lead to customer dissatisfaction.

In the local area networking space (i.e. networking within a building or a home), transmission rates are as high as 11 Mbps today. In the near future, these rates are expected to go up to around 54 Mbps. In the more distant future (e.g. in about 5 years), this rate is expected to be upwards of 100 Mbps. Thus, there is a disparity between local area wireless network (WLAN) system performance and wide area wireless network (WWAN) system performance in terms of access speeds. Using the above transmission rates, it can be seen that the difference in system performance is about 25 times faster in WLANs than in WWANs.

This has led to a problem for which a solution has not yet been found. The problem concerns how to provide high speed Internet access from all places beyond those traditionally in the domain of LANs (i.e. corporations and homes). For example, individuals often spend a great deal of time in public places such as airports, libraries, and restaurants. Yet, Internet access is not typically provided in these public areas. If Internet access is provided, it is typically tied to a particular ISP and the consumer really has no choices whatsoever concerning such things as quality of service, type of service available, and the like.

Accordingly, this invention arose out of concerns associated with improving network access so that a network, such as the Internet, can be accessed from a variety of places or locations at high speeds. In particular, the invention

1 arose out of concerns associated with enhancing Internet wireless connectivity
2 speeds in the wide area.

3

4 **SUMMARY**

5 Various embodiments pertain to enhancing wireless functionality, and
6 particularly to providing fast network access, e.g. Internet access, by pushing local
7 area wireless network system performance and functionality into the wide area
8 space. Wide area data networking data rates are much slower than local area data
9 networking rates. Aspects of the described embodiments exploit the higher data
10 rates that are available through the use of local area networks pushing this
11 functionality into the wide area space. Aspects of the described embodiments
12 have applicability in both wireless and wired networks.

13 In one embodiment, an architecture is provided, by one or more host
14 organizations, for providing individuals with fast wireless access to the Internet.
15 These networks are advantageously deployed in public areas such as airports,
16 shopping malls, libraries etc. The host organization may partition this network
17 either physically, or logically, into several smaller networks called subnets. Each
18 subnet may include a PANS (Protocol for Authentication and Negotiation of
19 Services) Server and a Policy Manager. A mobile user typically establishes a
20 communication link with the PANS server through an Access Point, and thereafter
21 wirelessly transmits and receives data to and from the Internet via the PANS
22 server. The positioning of the PANS server in the subnet is such that data traffic
23 from all users connected to this subnet goes through this server before reaching
24 any other network, including the Internet.

1 The PANS server is programmed to perform a number of different
2 functions in connection with providing network or Internet access. In one
3 embodiment, the PANS server ensures that users are authenticated to the system
4 before allowing them to send and receive data packets to and from the Internet. In
5 one aspect, authentication takes place through the use of an authentication
6 database. In one embodiment, the authentication database is a globally accessible
7 database and authentication takes place in a secure manner between the client and
8 the database (i.e. the PANS server is not privy to the exchange of the information
9 during authentication). In another embodiment, the authentication database is
10 available locally to the PANS server. After the global or the local database
11 authenticates the user, the user receives a unique token or key from the PANS
12 server. The user uses this token or key to identify himself or herself to the PANS
13 server in all subsequent data packet transmissions. All user data packets containing
14 this token or key, intended for the Internet, are allowed passage through the PANS
15 server.

16 In one embodiment, the user is given various choices concerning Internet
17 accessibility and the levels of service that are provided. For example, the PANS
18 server is programmed, in some embodiments, to negotiate with ISPs for Internet
19 access on behalf of users that are unaffiliated with an ISP. A user can define the
20 type of access they want (i.e. data rate, and perhaps the price they are willing to
21 pay), and the PANS server handles negotiation with the ISPs on the user's behalf.

22 In another embodiment, the PANS server provides flexible levels of
23 security for the user or client. For example, each user or client can be issued his or
24 her own key, dynamically generated by the PANS server, for use in encrypting
25

1 data packets that are transmitted to the PANS server. Each key can be of an
2 arbitrary length that is selectable by the user or the PANS server. In addition, the
3 PANS server can have a number of different encryption algorithms from which to
4 choose when a user is authenticated. Thus, a user can be handed a key having an
5 arbitrary length, and a randomly selected encryption algorithm to use when
6 encrypting their data packets.

7 In another embodiment, the PANS server is programmed to account for the
8 data packets that pass through it. Accounting for the data packets assists the
9 PANS server in charging clients for using the network, e.g. on a per packet or a
10 per byte basis, or a per transaction basis. In addition, accounting for the data
11 packets can help the PANS server in scheduling data packets for transmission.

12 In another embodiment, the PANS server is configured to provide the user
13 with an option to select a quality-of-service (QoS) level. Different costs can be
14 associated with different QoS levels. For example, a premium level can provide
15 the highest degree of security and a guaranteed amount of bandwidth. Other levels
16 might provide lesser degrees of security and lesser amounts of bandwidth. In one
17 aspect, the highest service level is available on a user-by-user basis where
18 individual users have a guaranteed a fixed amount of bandwidth and a very high
19 degree of security. Lesser levels of service are defined in terms of groups, where
20 each group contains a plurality of users. Bandwidth allocations in these groups
21 take place on a group basis, with members of the groups having to arbitrate for use
22 of the available allocated bandwidth. Each user is thus assured of receiving a fair
23 share of the associated allocated bandwidth.

1 In another embodiment, dynamic compression is utilized to ensure that data
2 packets are transmitted in an optimal manner. In the described wireless
3 embodiment, the PANS server (or the client) monitors the wireless medium for
4 transmission errors that might be caused by an obstruction in the line of sight
5 between the client and an access point. Whenever a pre-determined number of
6 errors are detected, measures are taken to lessen the degree of compression that is
7 utilized on the data packets. When the errors abate, the degree of compression is
8 increased. In effect, the amount of compression is modulated by the amount of
9 transmission errors that are detected during a sample period.

10 In another embodiment, a user interface is provided and provides feedback
11 to the user regarding their service level. Through the interface, the user can adjust
12 their quality of service level and observe a feedback mechanism that confirms
13 their quality of service level, i.e. actual bandwidth provided by the network.

14 In addition to the PANS Server, there exists a Policy Manager which
15 includes and manages various policies that determine the context of a particular
16 user's interaction with the network. For example, the Policy Manager can define
17 the level of service that a user receives, control access to host organization's
18 resources such as printers and fax machines etc., and the like. The Policy
19 Manager and the PANS server are communicatively linked so that the PANS
20 server can enforce the policies from the Policy Manager on a per user and per
21 connection basis.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a high level diagram of an exemplary system architecture in accordance with one embodiment.

Fig. 2 is a diagram of a computer system that can be used to implement various aspects of various embodiments.

Fig. 3A is a high level diagram of an exemplary wireless system architecture in accordance with one embodiment.

Fig. 3B is a high level diagram of an exemplary wireless system architecture in accordance with one embodiment.

Fig. 4 is a flow diagram that describes steps in a method in accordance with one embodiment.

Fig. 5 is a flow diagram that describes steps in a method in accordance with one embodiment.

Fig. 6 is a diagram of an exemplary user display in accordance with one embodiment.

Fig. 7 is a diagram that illustrates an exemplary quality of service embodiment.

Fig. 8 is a flow diagram that describes steps in a method in accordance with one embodiment.

Fig. 9 is a flow diagram that describes steps in a method in accordance with one embodiment.

Fig. 10 is a flow diagram that describes steps in a method in accordance with one embodiment.

Fig. 11 is a diagram of an error table that is utilized in accordance with one embodiment.

1 Fig. 12 is a diagram of a graphic user interface (GUI) in accordance with
2 one embodiment.

3

4 **DETAILED DESCRIPTION**

5 **Overview**

6 In the described embodiments, systems and methods are provided for
7 enhancing network access, e.g. Internet access, from any number of potential
8 locations that are not necessarily the traditional LAN locations, i.e. corporations or
9 homes. Individual users are given the opportunity to be mobile, yet connect with
10 the Internet using a very high speed location. In addition, users can be given
11 various choices that impact the level of service they are provided and the cost they
12 are charged for such service. Users can pay for such services by any suitable
13 method such as a credit card or a smart card based purchasing system. Access is
14 no longer necessarily tied inextricably to a particular employer or a particular ISP.
15 In various embodiments, flexibility and speed are enhanced through the
16 incorporation of a host organization network that makes use of wireless
17 communication. Users using mobile computing devices can wirelessly logon onto
18 the network and access the Internet. In the described embodiment, interfacing that
19 takes place with the user can be implemented as Web-based interfacing.

20 Fig. 1 shows a high level system diagram of an exemplary system
21 architecture generally at 100 that is capable of implementing various features
22 described below. Architecture 100 is used in connection with a computer network
23 an exemplary one of which is the Internet 102. One or more host organization
24 networks 104 are provided and are managed by a host organization. Examples of
25 a host organization include individual businesses that might, for example, be

1 located in a public area. Exemplary public areas include shopping malls, libraries,
2 airports, downtown shopping areas and the like. So, for example, the leftmost host
3 organization network 104 might be located in a shopping mall, while the rightmost
4 host organization network might be located in an airport. A plurality of service
5 providers can be incorporated in the architecture 100. In this example, the service
6 providers control access to the Internet and comprise a plurality of different
7 Internet Service Providers (ISPs) 105 that are communicatively linked with the
8 host organization network 104. Each host organization network 104 can include
9 one or more resources 106. Exemplary resources can include, without limitation,
10 scanners, tape drives, laser printers, and the like. Each host organization network
11 104 might also include a local authentication database 108 for purposes that will
12 be described below.

13 An authentication/negotiation component 110 is provided and is associated
14 with each host organization network 104. Although the authentication/negotiation
15 component 110 is shown as a combined component, it will be appreciated that
16 component 110 can be programmed to implement only one of an authentication or
17 negotiation function. Each of the components 110 is programmed/configured to
18 perform various functions that relate to providing users with network access.
19 Exemplary functions include authenticating the users, verifying the users during
20 subsequent communication, and negotiating various services from various service
21 providers for the user. In one particular embodiment, the verification function is
22 performed by a verification module that is positioned at each access module 112.
23 Providing a verification module at each access module is advantageous for quickly
24 detecting rogue users without allowing them any access further up the architecture
25 chain. As will be discussed below in more detail, the components 110 can

negotiate, on behalf of the users, with the different ISPs 105 for Internet access. In some embodiments, the users are given choices as to different levels of service that they can be provided. The levels of service can be associated with different fees that the user is charged, and can include different bandwidth allocations, security measures, and ISPs. These choices are then used by the authentication/negotiation components 110 to negotiate a desired level of service from one or more service providers, e.g. ISPs 105.

Sub A1

The architecture also includes a plurality of access modules 112 that are configured to enable a user to access the authentication/negotiation component 110. Although only one access module is shown for each authentication/negotiation component 110, more than one access module 112 can be provided for each authentication/negotiation component 110. Architecture 100 can also include a global authentication database 114 that is configured to be globally accessible from anywhere in the world. In the illustrated example, the global authentication database includes not only a repository of data or information that is used to authenticate users, but also any server computers or computing devices that are used in connection with the data repository to authenticate a user. The global authentication database 114 is advantageously accessible via the Internet 102. The global authentication database 114 can be any suitable globally accessible database that is capable of authenticating users as described below. Such databases can be operated by and/or associated with particular businesses, organizations or clubs for which authentication is desired. For example, a particular organization, e.g. Gold Club Frequent Fliers, may have negotiated with authentication/negotiation component 110 for Internet access for its members. When the members access the network 112 through the access

1 module 112, there needs to be a way to authenticate these Gold Club Frequent
2 Flyer members so that they can be provided Internet access at the negotiated level.
3 The global authentication database 114 provides a mechanism by which this can
4 be done, as will become apparent below. Alternately, the global authentication
5 database 114 can be a more generalized database that can be operated on behalf of
6 many organizations or businesses that might want to generally authenticate users.
7 An example of this type of global authentication database is Microsoft's Passport
8 Server and database. The MS server and database enable a user to be individually
9 verified against information that is maintained by the server and database. Often
10 times, this type of verification is conducted outside of the purview of other servers
11 ~~in an end-to-end secure fashion.~~

12 In the illustrated example, users can access the Internet through the use of a
13 client computer or computing device. In the context of this document, a "user"
14 refers to a human individual and a "client" refers to a computer or computing
15 device that the human individual uses to access the Internet. The client can be a
16 mobile computer such as a lap top computer, or can be any other suitable
17 computing device. The client can be provided by the host organization, or can be
18 a mobile computing device that travels with its particular user. When a user
19 wishes to access the Internet, they simply use their client computer to interface
20 with an access module 112. The access module permits communication with the
21 authentication/negotiation component 110. Authentication/negotiation component
22 110 first authenticates the user by using one of the local or global authentication
23 databases 108, 114 respectively. In the described embodiment, authentication
24 takes place outside of the purview of the authentication/negotiation component
25 110. For example, when the global authentication database 114 is used, the

1 authentication/negotiation component 110 permits the user to communicate
2 directly with the database 114. This communication can advantageously take
3 place using the Internet. In some embodiments, limited access to the Internet can
4 be granted by the authentication/negotiation component 110 for the limited
5 purpose of authenticating a user. After a limited period of time, if the user has not
6 been authenticated, Internet access can be terminated. For example, an IP address
7 might be temporarily granted to a user via a DHCP or NAT process. If the user
8 has not authenticated themselves within a definable period of time (e.g. ten
9 minutes), their internet access can be terminated. The database 114 takes the user
10 through a separate authentication process (e.g. entry of a user name and password)
11 so that the user can be authenticated to the database 114. This authentication
12 process can be a protected end-to-end secure process in which all of the user's
13 transmissions to the database 114 are encrypted from the client machine and can
14 be only decrypted by the database 114. An exemplary encryption technique is
15 Secure Socket Layer (SSL) transmission. Other secure techniques can be used.
16 This communication is secure from the authentication/negotiation component 110
17 and the host organization network 104.

18 Once the user is authenticated to the global authentication database 114, the
19 database 114 generates a message to the host organization network 104 and
20 informs the host organization network that the particular user has been
21 authenticated. After the authentication has occurred, all communication with and
22 access to the Internet takes place through the authentication/negotiation
23 component 110. That is, all of the data packets that are transmitted from and
24 received by the client are routed through the authentication/negotiation component
25 110.

1 An advantageous feature of the above architecture is that it enables a user to
2 freely move about from host organization to host organization, without having
3 their Internet access inextricably tied to any one particular ISP or to a particular
4 company such as their employer. This system permits a much more individual-
5 centric system that promotes user mobility, as will become apparent below.
6 Another advantage of this architecture is that once a user is authenticated, they can
7 move freely about without having to re-authenticate themselves to the system.
8 Another advantageous feature of the above architecture is that users can have
9 freedom of choice. That is, the authentication/negotiation component can be
10 programmed to negotiate for services on behalf of the user. For example, a host
11 organization network might have a number of different ISPs (e.g. AT&T, MCI,
12 Sprint and the like) that are under contract to provide Internet access. A user can
13 specify a particular level of service (i.e. transmission rate and desired cost
14 structure). The authentication/negotiation component then negotiates the desired
15 service level with the particular ISPs. Thus, a user can receive the best deal for
16 their desired parameters. As an example, a particular user may be in a rush (i.e.
17 between flights in an airport) and may need to have the fastest Internet access that
18 is possible. Further, they may be willing to pay a top premium for such access.
19 Once the authentication/negotiation component 110 is notified of these
20 parameters, it can then find the ISP that most closely meets the user's parameters.

21

22 **Exemplary Computer System**

23 Fig. 2 shows an exemplary computer system that can be used to implement
24 various computing devices, i.e. client computers, servers and the like, in
25 accordance with the described embodiments.

1 Computer 130 includes one or more processors or processing units 132, a
2 system memory 134, and a bus 136 that couples various system components
3 including the system memory 134 to processors 132. The bus 136 represents one
4 or more of any of several types of bus structures, including a memory bus or
5 memory controller, a peripheral bus, an accelerated graphics port, and a processor
6 or local bus using any of a variety of bus architectures. The system memory 134
7 includes read only memory (ROM) 138 and random access memory (RAM) 140.
8 A basic input/output system (BIOS) 142, containing the basic routines that help to
9 transfer information between elements within computer 130, such as during start-
10 up, is stored in ROM 138.

11 Computer 130 further includes a hard disk drive 144 for reading from and
12 writing to a hard disk (not shown), a magnetic disk drive 146 for reading from and
13 writing to a removable magnetic disk 148, and an optical disk drive 150 for
14 reading from or writing to a removable optical disk 152 such as a CD ROM or
15 other optical media. The hard disk drive 144, magnetic disk drive 146, and optical
16 disk drive 150 are connected to the bus 136 by an SCSI interface 154 or some
17 other appropriate interface. The drives and their associated computer-readable
18 media provide nonvolatile storage of computer-readable instructions, data
19 structures, program modules and other data for computer 130. Although the
20 exemplary environment described herein employs a hard disk, a removable
21 magnetic disk 148 and a removable optical disk 152, it should be appreciated by
22 those skilled in the art that other types of computer-readable media which can
23 store data that is accessible by a computer, such as magnetic cassettes, flash
24 memory cards, digital video disks, random access memories (RAMs), read only
25

1 memories (ROMs), and the like, may also be used in the exemplary operating
2 environment.

3 A number of program modules may be stored on the hard disk 144,
4 magnetic disk 148, optical disk 152, ROM 138, or RAM 140, including an
5 operating system 158, one or more application programs 160, other program
6 modules 162, and program data 164. A user may enter commands and
7 information into computer 130 through input devices such as a keyboard 166 and a
8 pointing device 168. Other input devices (not shown) may include a microphone,
9 joystick, game pad, satellite dish, scanner, or the like. These and other input
10 devices are connected to the processing unit 132 through an interface 170 that is
11 coupled to the bus 136. A monitor 172 or other type of display device is also
12 connected to the bus 136 via an interface, such as a video adapter 174. In addition
13 to the monitor, personal computers typically include other peripheral output
14 devices (not shown) such as speakers and printers.

15 Computer 130 commonly operates in a networked environment using
16 logical connections to one or more remote computers, such as a remote computer
17 176. The remote computer 176 may be another personal computer, a server, a
18 router, a network PC, a peer device or other common network node, and typically
19 includes many or all of the elements described above relative to computer 130,
20 although only a memory storage device 178 has been illustrated in Fig. 2. The
21 logical connections depicted in Fig. 2 include a local area network (LAN) 180 and
22 a wide area network (WAN) 182. Such networking environments are
23 commonplace in offices, enterprise-wide computer networks, intranets, and the
24 Internet.

When used in a LAN networking environment, computer 130 is connected to the local network 180 through a network interface or adapter 184. When used in a WAN networking environment, computer 130 typically includes a modem 186 or other means for establishing communications over the wide area network 182, such as the Internet. The modem 186, which may be internal or external, is connected to the bus 136 via a serial port interface 156. In a networked environment, program modules depicted relative to the personal computer 130, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

Generally, the data processors of computer 130 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems are typically distributed, for example, on floppy disks or CD-ROMs. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described below in conjunction with a microprocessor or other data processor. The invention also includes the computer itself when programmed according to the methods and techniques described below.

For purposes of illustration, programs and other executable program components such as the operating system are illustrated herein as discrete blocks, although it is recognized that such programs and components reside at various

1 times in different storage components of the computer, and are executed by the
2 data processor(s) of the computer.

3

4 **Exemplary System Architecture**

5 Fig. 3A shows an exemplary system architecture 100 that includes a
6 wireless network feature. Although the discussion that follows is in the context of
7 a network that includes the illustrated wireless feature, it is to be understood that
8 the system architecture could, alternately, employ a wired network in substitution
9 for the wireless network feature that is described below. In the discussion that
10 follows, like numerals from the Fig. 1 example are utilized where appropriate,
11 with differences being indicated with the suffix “a” or with different numerals.

12 In the illustrated example, multiple wireless nodes are provided. Each
13 wireless node is constituted by an individual client. In the example, two clients or
14 wireless nodes are shown, although in actuality, many wireless nodes would
15 typically be employed. Each client computer typically has a network card
16 installed therein which permits wireless communication. The wireless
17 communication takes place through the use of known wireless techniques that will
18 be apparent to those of skill in the art. Accordingly, these techniques are not
19 discussed further. The client can comprise any suitable computing device which,
20 in this example, is configured for wireless communication. Each of the wireless
21 nodes is connected through an access module 112a. In the wireless example, each
22 access module 112a comprises one or more access points 306 that permit wireless
23 access in known ways using known protocols. In the illustrated example, all the
24 access points 306, for a particular access module 112a, together constitute a single
25 wireless subnet. This is advantageous from the network standpoint because of

1 routing issues. For example, every subnet on the Internet is identified by a unique
2 number. Every client connected to this subnet uses this number as part of its own
3 unique identification. In the Internet, a subnet number is an integral part of the
4 client's unique IP address. Various routers that are used in the network
5 environment use the subnet portion of the IP address to determine where to route
6 various data packets. When a client changes its subnet, its IP address also
7 changes. By having all of the access points 306 in an access module that is
8 associated with a single subnet, an individual is free to move between access
9 points of the same subnet without having to change their IP address. This is
10 particularly advantageous when the host organization network is located in a
11 public place. For example, an individual may be traveling through a large airport
12 in which a host organization network has been deployed. They may use a
13 particular access point to access the Internet immediately upon disembarking from
14 a plane. The individual can continue to stay connected to the Internet even as they
15 move into different locations of the airport serviced by different access points 306.
16 Because the user still accesses the Internet through the same wireless subnet, they
17 need not be issued a different IP address. This further enhances the robustness
18 and speed of the system. Access module 112a may or may not communicate
19 wirelessly with authentication/negotiation component 110a.

20

21 **Authentication/Negotiation Component**

22 In the illustrated example, authentication/negotiation component 110a
23 comprises a server 302 (referred to herein as a "Protocol for Authentication and
24 Negotiation of Services" or "PANS" server) and a Policy Manager 304. The
25 PANS server 302 may or may not be configured to receive wireless

1 communication from access module 112a. The authentication/negotiation
2 component 110a is communicatively linked with the host organization network
3 104. Any suitable communication link can be used. In various embodiments,
4 such link can comprise a high speed wired connection or a wireless connection.
5 The host organization network 104 is communicatively linked to the Internet 102
6 and, in some embodiments to ISPs 105 through conventional network systems.

7 The PANS server 302 is a software component that is designed to
8 implement various functionalities that are described below. In the illustrated
9 example, the PANS server 302 is programmed to handle all of the authentication
10 issues and the negotiation of services for a particular user. In operation, all of a
11 user's Internet data packet traffic (to and from) is routed through the PANS server
12 302. This is advantageous for a number of different reasons among which are
13 included data packet accounting (e.g. for billing purposes), and traffic control (e.g.
14 for administering user-selected quality of service levels).

15 The Policy Manager 304 is a software component that is responsible for
16 managing the various policies that are used by the PANS server 302 in providing
17 services to the different clients.. The Policy Manager 304 can contain one or more
18 policy tables that define various resource access policies (e.g. which users can
19 access local resources 106 and what is the level of access), network access speeds,
20 security levels and the like. For example, a corporation such as Microsoft might
21 negotiate a service package with a particular host organization network that has a
22 wireless network with Internet access deployed in the Seattle-Tacoma (SeaTac)
23 airport. The negotiated package provides that for any Microsoft employee, the
24 host organization would allow, free of charge, a certain service level. Service
25 levels above the negotiated service level may cost the employee a nominal charge.

1 The Policy Manager 304 then maintains an entry in its policy table that indicates
2 that Microsoft employees are to be granted free access to the host organization's
3 network at the negotiated level. Accordingly, when any Microsoft employee logs
4 onto the SeaTac network, the Policy Manager 304 indicates to the PANS server
5 302 that access for this user at the negotiated service level is to be free of charge.
6 Accordingly, the PANS server 302 interacts with the Policy Manager 304 to
7 decide which of the client's packets will be allowed passage to the Internet and
8 how they will be scheduled for transmission. In addition, data packets from the
9 client also pass through the PANS server 302 before they are allowed to be
10 transmitted to the host organization's network, e.g. the host organization's
11 intranet.

12 In one aspect, the Policy Manager 304 is a distributed Policy Manager
13 where the policies that are provided by the Policy Manager are not locally
14 verifiable. As an example, consider the following: The Policy Manager 304 can
15 contain many different policies that govern or regulate Internet access for many
16 different classes of individuals. For example, Boeing may have negotiated for a
17 quality of service level 1 (discussed below in more detail) for all of its employees.
18 There may also be a policy that governs or regulates Internet access for members
19 of certain clubs, i.e. the Gold Club Frequent Fliers. Having to locally verify the
20 authenticity of users claiming to be Boeing employees and/or members of the
21 Gold Club Frequent Fliers could be a daunting task, although it could be done. A
22 much better approach is to verify the authenticity of these users using one or more
23 globally accessible authentication databases. For example, both Boeing and the
24 Gold Club Frequent Fliers may have their employees (members) registered with a
25 central globally accessible authentication database such as MS Passport. In this

case, when a user logs into the system, the authentication/negotiation component 110a passes the user to the database, e.g. via a hyperlink, for authentication. After the user is properly authenticated, the authentication/negotiation 110a provides Internet access at the negotiated service level. In some embodiments, and particularly where a user may be a member of more than one club or organization for which a service level has been negotiated, the authentication/negotiation component 110a can select the club or organization that provides the better quality of service level for the user. The authentication/negotiation component 110a can then pass the user to the appropriate authentication database so that the user can be authenticated for the particular selected club or service level. Once authenticated for the particular club or service level, Internet access can be provided by the authentication/negotiation component 110a in accordance with the negotiated service level.

Sub A2

> ~~The authentication/negotiation component 110a can also include (although it is not specifically shown) a dynamic host configuration protocol (DHCP) server that is responsible for issuing and managing IP addresses. DHCP servers are known and will not be further discussed herein. Alternatively, the authentication/negotiation component 110a can include a Network Address Translator (NAT) software module. NAT is responsible for issuing private addresses to clients and then translating these to public routable IP addresses. NAT is also known and will not be further discussed herein.~~

Sub A3

> ~~In the illustrated example, a global authentication database 114a is provided in the form of Microsoft's Passport Server. As pointed out above, any suitable global database can be used. This global authentication database 114a can comprise multiple different machines that are located globally around the world.~~

1 The database is used, in one embodiment, to authenticate users as will be
2 described in the "Authentication" section just below.

3

4 **Alternate Architecture**

5 Sub A4 > Fig. 3b shows an alternate architecture in which the host organization
6 subnet comprises a authentication/negotiation component 110b that includes a
7 PANS Authorizer 302b and a policy manager 304a. The PANS Authorizer 302b
8 authenticates users just as described above. In this particular architecture, the
9 verification functionality is shifted to the access modules 112b in the form of a
10 PANS verifier module 308 that resides at one or more of the access points of the
11 access module. In the illustrated example, a PANS verifier 308 resides at each of
12 the access points. The advantages of providing a PANS verifier at each access
13 point include the detection of rogue users early on before they access the system.
14 That is, once a user is authenticated, the PANS Authorizer 302b passes the
15 verification function to the PANS verifier 308 at one or more of the access points.
16 Thus, whenever a user attempts to send a data packet to the Internet, they are
17 verified at the access module before the packet is transmitted to the
18 authentication/negotiation component 110b. If a rogue user attempts to transmit
19 an unauthorized packet, the packet can be detected very early in the architecture
20 chain.

21

22 **Authentication**

23 In the described embodiment, individual authentication is provided for each
24 of the users. This can be done in a manner that is independent of any affiliation
25 that the user might have, such as an employer affiliation or an ISP affiliation, thus

1 providing an individual-centric approach to authentication. In this example, a user
2 is simply authenticated to the system architecture. The system architecture then
3 takes over and provides the user with different options for accessing the Internet.

4 Fig. 4 is a flow diagram that describes steps in an authentication method in
5 accordance with the described embodiment. The description that is given just
6 below is given in the context of the architecture that is shown in Fig. 3A.

7 Step 400 establishes a link between a user and an access point 306. This
8 step can be accomplished by a user physically traveling to a location that is within
9 transmission range of the access point. As an example, a shopping mall owner
10 might have a deployed wireless network that includes one or more access points
11 306. A user might bring their own configured computing device (i.e. laptop) to
12 the mall, or might use a mall-provided computing device. The user then
13 establishes a wireless communication link with the access point 306. The wireless
14 link can be established through the use of any suitable techniques. The
15 communication link need not, however, be a wireless link as pointed out above.

16 Once the link is established, step 402 displays a user interface under the
17 influence of a browser that is executing on the client computing device. The user
18 interface welcomes the user to the wireless network and provides a mechanism
19 through which the user can be authenticated to the system. This can be done in a
20 number of different ways. For example, the user may click on an icon to see a list
21 of member organizations for which various service levels have been previously
22 negotiated. The user then selects one or more of the organizations to which they
23 belong. The authentication/negotiation component 110a can then select a user-
24 designated organization whose plan offers the best Internet access and then
25 authenticate that user for that particular organization as described above.

1 Any suitable authentication method can be used. In the illustrated example,
2 it has been found particularly advantageous to authenticate the user in a manner
3 that provides end-to-end security between the user and the authenticating entity.
4 In this example, a global authentication database 114a is utilized as the
5 authenticating entity to authenticate the user. Accordingly, step 404 provides a
6 secure link between the user or client machine and the global authentication
7 database 114a. The secure link can be established by having the user click on a
8 browser page icon that links the user to the authentication database 114a. One
9 example of a secure link can be one that is established through the use of Secure
10 Socket Layer (SSL) techniques. By authenticating the user in this manner, the
11 user's authentication information is encrypted before it leaves the client machine.
12 This means that the authentication/negotiation component 110a is unable to
13 ascertain any of the user's authentication information, e.g. the user's password and
14 the like. This provides a very high degree of security and greatly reduces the
15 chances that a user's protected information will be compromised. The user's
16 information can then only be decrypted by the authenticating authority which, in
17 this example, is the MS Passport Server 114a. Authenticating the user in this
18 manner greatly improves upon systems that authenticate a user by serving as a
19 proxy for the user.

20 Once a secure link is established between the user and the global
21 authentication database, step 406 authenticates the user to the global
22 authentication database. This step can be implemented by displaying a suitable
23 logon web page for the user in which they provide their user name and password
24 for the global authentication database. Once the global authentication database
25 confirms the user's information, the user is authenticated.

At this point, when the user has been authenticated to the global authentication database, communication can now take place in the background between the global authentication database 114a and the PANS server 302. Specifically, step 408 notifies the authentication/negotiation component 110a, i.e. the PANS server 302, that the user has been authenticated. This step can be implemented by having the global authentication database generate a message and send it to the PANS server 302. Once the PANS server receives the notification, it can then, if necessary, receive any additional information about the user that it needs. For example, the global authentication database 114a might contain the user's credit card information or other information that can be utilized to bill the user (e.g. billing address etc.). Accordingly, step 410 determines whether any additional information is needed about the particular user. If additional information is needed, then the PANS server 302 receives the information (step 412) from the global authentication database 114a. If no additional information is needed, or in the event that any needed information is received, step 414 generates a unique token for the user. In the illustrated and described example, the PANS server 302 generates a unique token or key for each of the individual users. Step 416 then provides the user token or key to client machine for use during the user's session. Specifically, the token or key is used by the client computer each time a data packet is sent to the Internet via the PANS server 302. The token or key assists the PANS server 302 in identifying data packets from authenticated users. Specifically, the PANS Server 302 maintains a list of tokens that have been distributed to authenticated users. On receiving a data packet with an embedded token, the PANS server 302 checks the list to determine whether a particular token is valid. If a token is determined to be invalid, then the PANS server 302 can

refuse to further transmit the data packet into the Internet or the host organization's intranet. The PANS server 302 can be used to allow only those data packets which contain a valid token.

As a further added degree of security, each token or key that is used by a particular user is encrypted so that unscrupulous users cannot steal another user's token. In this example, only the client computer and the PANS server know the particular user's token or key. Any suitable encryption techniques can be used to encrypt the user's token.

Security

In addition to providing end-to-end security, as in the case of user authentication, other additional security measures can be provided to protect the communication that takes place between the PANS server 302 and the client.

In the described embodiment, after the user is authenticated, the PANS server 302 can issue the user a key. Advantageously, each user is issued a different key. This key can be transported to the user using secure transport protocols, e.g. https. The client then adds this key to each outgoing data packet, uses the key to encrypt the resulting packet, and then transmits it to the PANS server 302. On receiving the encrypted data packet, the PANS server decrypts the packet and checks the embedded key for validity. If the key is valid, the PANS Server 302 removes the key from the data packet, and then passes the data packet on to the Internet. If the PANS server 302 finds a invalid key in the packet, it simply drops the packet without forwarding it on to the Internet. The ability of the PANS server 302 to dynamically generate a key for each user constitutes an improvement over other network systems that utilize a fixed number of keys for a

1 variable number of users. In those systems there might be, for example, four or
2 five keys that are allocated for use among numerous different users. Thus, a
3 plurality of different users will use the same key to encrypt their data. If one of
4 the fixed keys is broken for one particular user, then the data that is associated
5 with all of the other users who share that key can be compromised as well. In the
6 present case, breaking the key for one user carries with it no implications insofar
7 as other users are concerned.

8 In another aspect, the keys that are issued by the PANS server 302 can have
9 an arbitrary length. For example, key lengths can be selected to be 40 bits, 128
10 bits, or 256 bits in length. Selection of the key length might take place randomly.
11 Alternately, a user may be able to select the length of key that is used.
12 Alternately, the user might select from a number of quality of service levels that
13 each provide different length keys in accordance with varying degrees of security.
14 For example, a user may have information that is only generally sensitive. In that
15 case, a smaller key length may be in order to protect the information. Alternately,
16 a user might have information that is highly sensitive. In this case, a longer key
17 length may be in order. As will be appreciated by those skilled in the art, the
18 length of a key is proportional to the computational overhead that is necessary to
19 process the key. The same relationship holds true for the computational overhead
20 that is required to break the key. In one aspect, the user may be presented with
21 different payment options that are associated with the varying degrees of security.
22 For example, for a small fee, a key length of 40 bits might be purchased. For a
23 somewhat larger fee a 128-bit key might be purchased. For an even larger fee, a
24 256-bit key might be purchased. Thus, in this example, a user can purchase
25

1 various degrees of security that protect their communication with the PANS
2 server.

3 In yet another aspect, varying degrees of encryption can be provided to
4 further enhance security. In this case, a user might be able to select from among
5 options that provide for no encryption to a very high level of encryption. For
6 example, the highest level of encryption might involve encrypting an entire data
7 packet. A lesser level of encryption might involve encrypting only the header of
8 each data packet or only a portion of the body of each data packet.

9 In yet another aspect, flexible security measures are provided in the form of
10 multiple different encryption/decryption algorithms that are available for selection
11 by the PANS server 302. For example, the PANS server 302 may have a number
12 of different encryption algorithms, e.g., five or six different encryption algorithms
13 from which it can select. When the server issues a key to a user or client, it can
14 also designate which of the five or six algorithms to use for encryption. Thus, the
15 server 302 can randomly assign an encryption algorithm to the client. In one
16 aspect, the different encryption algorithms might be differently priced depending
17 on the complexity of the encryption. In this case, the different encryption
18 algorithms might be incorporated in the different service level packages that are
19 discussed in more detail below.

20 Each of these additional aspects provides a robust security environment for
21 the communication that takes place between the client and the PANS server 302.
22 In the wireless embodiment this is particularly advantageous because of the
23 openness with which the communication between the client and the PANS server
24 302 takes place, and its susceptibility to eavesdropping. One or more of these
25 additional aspects can be combined for a particularly robust combination of

1 security measures. For example, in addition to each user having a randomly
2 generated key, certain users may have a key length of 40 bits, while other users
3 have a key length of 128 bits. Further, users may also, in addition to having
4 variable length keys, have different encryption algorithms as between them.
5 Further, the different security measures can be grouped into different quality of
6 service levels that can be purchased by a user, as will be discussed below in more
7 detail.

8 Fig. 5 is a flow diagram that describes steps in a security process in
9 accordance with the described embodiment. The processing that is described just
10 below further embellishes steps 414 and 416 of Fig. 4. Various steps that are
11 described by Fig. 5 are implemented by the PANS server 302 and the client. Fig.
12 5 designates the steps that are performed by the PANS server 302 by setting them
13 forth on the left side of the flow diagram. Likewise, the steps that are performed
14 by the client are set forth on the right side of the flow diagram.

15 Step 500 presents one or more security options to a user. This is done by
16 displaying on the client machine a page that specifies the various security options.
17 For example, a user may elect to use no security or may select from among a
18 number of different levels of security. Fig. 6 shows an exemplary page 600 that
19 can be displayed on the client machine. There, a user is given an opportunity to
20 select from among a number of different key lengths. Page 602 shows another
21 security option that enables a user to select the number of encryption algorithms
22 from which a single algorithm will be selected for use. The key length, number of
23 encryption algorithms, and encryption level (header only versus entire packet) can
24 be tied to a fee that is paid by the user.

25

Step 502 selects a security option. Step 504 determines which security option has been selected by the user. Once the PANS server 302 determines the security option, step 506 generates a key and step 508 issues the key to the user or client machine using a secure https session. When the key is issued to the user, if appropriate, the client machine will also be notified as to which particular encryption algorithm to use in connection with the issued key. Step 510 receives the issued key. Subsequently, each time the client machine generates a data packet, this key is added to the packet and the resulting packet is encrypted with the key (step 512). Step 514 then transmits the encrypted data packet to the PANS server 302. Each data packet that is received by the PANS server is then decrypted, the key is extracted and checked for validity. If the key is valid the packet is allowed passage into the host organization's Intranet or into the Internet as appropriate.

Quality of Service

In one embodiment, multiple service levels are provided and are available to each user. A user can be given an opportunity to purchase a certain service level. Alternately, the user might be a member of one or more organizations that have arranged for a certain service level on behalf of their members.

Each service level can provide the user with a bundle of services that fit that particular user's needs. Each service level can have one or more services associated with it. These services can be provided in varying degrees between the different service levels. As an example, consider that there are three service levels that are available to a user—Level I (premium service), Level II (enhanced

1 service) and Level III (basic service). The premium service level is the most
2 expensive, followed by the enhanced service level and the basic service level.

3 Fig. 7 diagrammatically illustrates the three exemplary service levels. In
4 this particular example, the Level I premium service is provided to individual
5 users on a per node (per user) basis. In this example, each of the individual users
6 is guaranteed a certain portion of bandwidth for their data packet transmissions. In
7 addition, the service level can have a degree of security associated with it. In this
8 example, the premium service level might have the highest degree of security,
9 examples of which are given above in the "Security" section. Each of the
10 additional service levels (enhanced and basic) is provided on a class basis. That is,
11 users that opt to purchase or are provided these levels of service are aggregated
12 into a user group. Each user group is then assigned a portion of bandwidth and
13 perhaps a security degree. Each group is then responsible for arbitrating amongst
14 its members for the available bandwidth. In this example, the enhanced Level II
15 service group has a smaller number of group members than the basic Level I
16 service group. In the illustrated quality of service embodiment, each user is given
17 a fair share of the available bandwidth.

18 As an example, consider that in exchange for paying a service fee, Level I
19 users are given individual reservations slots that individually guarantee an amount
20 of bandwidth, e.g. 200 Kbps. Level II users, as a group, also receive a guarantee
21 of available bandwidth, e.g 200 Kbps. The individual group members must,
22 however, allocate the bandwidth between them when it is their turn to transmit
23 their data packets. Level III users receive the same guarantee as the Level II users,
24 except that there are more users that must arbitrate for available bandwidth.
25

1 The inventive scheduling techniques provide a user-based scheduling
2 system that greatly improves upon previously-used “flow-based” scheduling. In
3 flow-based scheduling, streams of packets or “flows”, are received from several
4 computers. The flows typically originate from different applications. A single
5 user may be executing more than one application that is producing and consuming
6 a flow. A router typically evaluates the flows that it receives, and then attempts to
7 allocate a fair share of the bandwidth among the different flows. Flow-based
8 quality of service systems emphasize the flows and do not regard the source of the
9 flows. For example, in a flow based system, it may be possible for one user with
10 many different flows to consume all of the available bandwidth to the exclusion of
11 the other users. The inventive user-based service system is different from the
12 flow-based system because it makes its distinctions based on the users or user
13 groups. In this way, the quality of service is improved for all flows, not just for
14 the one flow that might happen to be usurping the available bandwidth. Amongst
15 the individual users, flow based scheduling can, however, take place, e.g. by a user
16 designating which of their flows should have priority. However, as between the
17 individual users scheduling is accomplished on a user basis.

18 There are many ways that the above quality of service system can be
19 implemented. In one embodiment, the quality of service system is implemented
20 by the PANS server 302 as follows. Once all of the users have selected their
21 quality of service levels, the PANS server 302 monitors the available bandwidth
22 and generates a signal or message that is transmitted to the users when it is their
23 turn to transmit their data packets. The users can select their quality of service
24 level by purchasing the service level. Alternately, the quality of service level
25 might be provided to the user as part of a package that was negotiated by an

organization or employer on behalf of the user. Regardless, once the service level has been selected and the user authenticated, the PANS server 302 can transmit a “go” signal to an individual member of the Level I group when it is their turn to transmit. When the individual member receives the “go” signal, they can then begin to transmit their packets if they have any to transmit. Based upon the user token that is included with each packet transmission from the user, the PANS server 302 will be able to verify that the packet transmission is coming from the appropriate user and is therefore valid. After the individual user has transmitted enough of its packets, the PANS server notifies the user that its transmission time is over and then sends a “go” signal to another user or group. It is important to note that the PANS server can be programmed to monitor for packet traffic after the packets have left the sender. Monitoring the packet traffic can ensure that a user’s packets have actually been transmitted to the Internet and are not sitting in a queue awaiting transfer. That is, in this case, the PANS server is programmed and can intelligently figure out in a real world sense whether the packets that have been provided by a user have actually been transmitted to the Internet so that they will not, at some time downstream, interfere with another’s data packets. Assume for example, that 20 milliseconds of transmission time has been allocated among three users in the following amounts: 5 milliseconds (user 1), 5 milliseconds (user 2) and ten milliseconds (user 3). Assume also that user 1’s transmission actually takes 6 milliseconds and user 2’s transmission actually takes 7 milliseconds. That would mean that only 7 milliseconds of the total 20 milliseconds of transmission time are available for user 3. In this case, the PANS Service can monitor the packet transmission from the other users and can automatically and in a dynamic fashion adjust the allocation for user 3 to 7 milliseconds. When a group such as

1 the Level II group receives a "go" signal, the group must then begin an arbitration
2 sequence to arbitrate among the various group members for packet transmission.
3 Arbitration may, however, be conducted in advance of receiving the "go" signal.
4 Any suitable arbitration scheme can be used.

5 > ~~Fig. 8 shows a flow diagram that describes steps in a quality of service~~
6 method in accordance with the described embodiment. Some of the illustrated
7 steps can be implemented by the PANS server 302, while other of the steps can be
8 implemented by the client. Step 800 displays one or more service level options for
9 a user. In the described embodiment, the service level options can be displayed on
10 the client machine so that the user can select an appropriate level. For example, if
11 a user is in a busy airport and is between flights, they may only have a limited
12 amount of time to transact their on line business. In this instance, the user may
13 select the premium Level I service level so that they have the best chance of
14 transacting their business. The service level options might also be displayed in the
15 form of a list that describes various member organizations that have negotiated for
16 particular service levels on behalf of their members. Step 802 selects a service
17 level option. This step can be implemented by the user selecting a particular
18 displayed service level. Alternately, the user can select from among the groups
19 that are described in the list of member organizations. After the user has been
20 authenticated, step 804 monitors the data packet traffic that is generated from all
21 of the users. Step 804 is typically a continuously implemented step in which the
22 data packet traffic is monitored as users are added to and deleted from the
23 collection of users that are transmitting data packets at any particular time. In this
24 example, since all of the data packets from each of the users or clients gets routed
25 through the PANS server, it is in the best position to oversee, monitor and control

1 the packet flow. The PANS server then, in accordance with its programming
2 instructions, generates a "go" signal when a user or group of users is authorized to
3 transmit their data packets. Steps 808 and 810 wait to receive the "go" signal.
4 Once the "go" signal is received, if the authorized recipient is an individual user
5 (step 812), then they can begin their data packet transmission. If the authorized
6 recipient comprises a group of users (e.g. Level II or III users), they can begin
7 their arbitration process (step 816).

8

9 **Accounting**

10 In one embodiment, PANS server 302 implements an accounting function.
11 That is, because all of the data packets get routed through the PANS server, it is in
12 the best position to maintain an accounting of the packets that its sends and
13 receives. By accounting for all of the data packets, the PANS server can ensure
14 that users are billed for an accurate amount of bandwidth that they may have
15 consumed. To do this, the PANS server may be communicatively linked with a
16 billing database that is not specifically illustrated. The PAN server then
17 communicates the particular user's use parameters (i.e. amount of time spent on
18 the network, number of data packets transmitted/received, etc.) to the billing
19 database which can then ensure that the user is billed an appropriate amount.

20 As an example, consider that billing is based on the number of packets that
21 pass through the PANS server 302. When the PANS server sends a "go" signal to
22 a particular user, if the user transmits only a small number of data packets, then in
23 this example, the billing charge should be a small charge. Alternately, consider
24 that the billing is based on the total amount of bits that are transmitted. The PANS
25 serve 302 keeps track of the number of bits that are transmitted by the user and

1 sees that the user is billed accordingly. Further consider that the billing is based
2 on the amount of time an individual spends using the network. In this case, the
3 PANS server can keep an accounting of the time so that the user can be billed
4 accordingly. In addition, the PANS server can be configured to monitor a user's
5 use of local resources, e.g. printers, scanners and the like. Accordingly, the PANS
6 server can see that users are billed for the amount of the resource that they
7 consume. It will also be appreciated that the PANS server can use its accounting
8 feature to efficiently schedule users for data packet transmission.

9 Accounting for the data packets is also advantageous from the standpoint of
10 assessing the collective system demand of members of various organizations that
11 might have negotiated service level packages for their members. For example, if a
12 particular organization's members placed an unusually high burden on the system
13 that is not commensurate with the organization's negotiated service level, then
14 measures might be taken to bring the burden in line with the negotiated service
15 level. This might involve charging the organization a higher fee for its negotiated
16 service level. It might also involve changing the organization's service level.

17 Fig. 9 is a flow diagram that describes steps in an accounting method in
18 accordance with the described embodiment. Step 900 monitors the use of the host
19 organization network. This step is most advantageously implemented by the
20 PANS server 302. The PANS server can monitor the network use in a number of
21 different ways. For example, the PANS server can monitor the packet traffic or
22 the time that is spent on the network by the individual users. Step 902 collects
23 information that pertains to the user's use of the network. Here, such information
24 can include, without limitation, the total number of packets that are transmitted by
25 a user, the total number of bytes that are transmitted by a user, or the total number

1 of minutes that a user spends logged onto the network to name just a few. Once
2 this information is collected by the PANS server, step 904 uses the information to
3 charge the user for its network use. This step might be implemented by having the
4 PANS server communicate the collected information to a billing server that
5 receives the information and then generates a bill for the user.

6

7 Dynamic Compression

8 In one embodiment, dynamic data compression is utilized as a way to
9 optimize data packet transmission. Dynamic data compression is particularly
10 useful in the wireless embodiments for the following reasons. One way to
11 enhance the use of available bandwidth is to compress the data that is being
12 transmitted. By compressing the data, more data can be sent from the client to the
13 PANS server and vice versa. In the wireless embodiment, there are certain error
14 conditions that can occur that can corrupt the transmission of data packets. For
15 example, if there is good line of sight between the client and the appropriate
16 access point, then the chances of having a corrupted transmission is less likely
17 than if there is an object that blocks the transmission pathway between the client
18 and the access point. Consider, for example, a host organization network that is
19 deployed in a shopping mall. There may be times when the amount of human
20 traffic through the mall disrupts the transmission signals between the client and the
21 access point, or between the access point and the PANS server. In these instances,
22 it is highly desirable to curtail somewhat the amount of compressed data packets
23 that are being sent. This follows logically from a realization that corruption events
24 that corrupt compressed data are more destructive than corruption events that
25 corrupt uncompressed data because in the former case, more data gets corrupted.

1 Fig. 10 is a flow diagram that describes steps in a dynamic compression
2 method in accordance with the described embodiment. Dynamic compression can
3 be performed by both the PANS server and the client machine. Step 1000 defines
4 an event window within which monitoring takes place. The event window can be
5 any suitable time frame for which monitoring is desired. Step 1002 monitors for
6 errors that occur within the event window. The errors that can be monitored for
7 include, without limitation bit errors, packet errors and the like. Monitoring can
8 take place using any suitable monitoring techniques as will be understood by those
9 of skill in the art. Accordingly, monitoring techniques are not discussed in detail
10 any further. Step 1004 determines whether the errors that occur are greater than a
11 predetermined amount. Errors can be accounted for in any suitable way. For
12 example, the gross number of errors that occur in a given time period can be
13 determined. Alternately, the error rate can be determined. During this time, a base
14 line compression can be employed by the client and the PANS server. A base line
15 compression can comprise using a certain compression algorithm or variation
16 thereof. In addition, a base line compression can comprise compressing a certain
17 amount of the data packets (e.g. a certain percentage) within the event window. If
18 the errors exceed the predetermined amount, then step 1006 implements dynamic
19 compression. Additionally, when a certain predetermined amount of errors is
20 reached, Forward Error Correcting codes can be used. Forward Error Correcting
21 codes will be understood to those of skill in the art and are therefore not discussed
22 in any detail here.

23 When dynamic compression is implemented, its goal is to compress less of
24 the data during a time period when there are more detected errors. This can be
25 done in a number of different ways. For example, when an error threshold is

1 exceeded, a different compression algorithm might be used. Alternately, when an
2 error threshold is exceeded a lower percentage of data packets within the event
3 window might be compressed using the same compression algorithm.

4 Fig. 11 shows a look up table generally at 1100 that can be used, in one
5 embodiment, to implement dynamic compression. Here, the look up table 1100
6 contains two fields—an error field and a compression percent field. In this
7 example, there are 5 entries in the error field, i.e. 0-1, 2-5, 6-10, 11-15, +15.
8 These entries constitute different thresholds for errors that can occur within the
9 event window. Each of the entries in the error field is associated with a
10 compression percent. In this example, the compression percentages range from
11 100% for when there are very few detected errors, to 0% for when there are a large
12 number of detected errors. Accordingly, as the data packets are transmitted, as
13 long as the detected errors in an event window do not rise above 1, all of the data
14 packets in the event window will be compressed. If, for example, the detected
15 errors rise to between 6-10, then the percentage of data packets that get
16 compressed drops to 50%. This helps to ensure that during periods of
17 transmission disruption, less of the data that is transmitted between the PANS
18 server and the client are compressed thereby reducing the amount of data that is
19 ultimately corrupted.

20

21 **User Interface**

22 Fig. 12 shows an exemplary graphic user interface generally at 1200.
23 Interface 1200 is configured for display on a client computing device. In this
24 example, the interface 1200 includes a bandwidth selector 1202 that is configured
25 to enable a user of the computing device to adjust the bandwidth that is allocated

1 to the computing device. Accordingly, a user is given the choice of the bandwidth
2 allocation that they can receive. Interface 1200 also includes a cost selector 1204
3 that is configured to enable a user of the computing device to adjust the cost that is
4 associated with the bandwidth that is allocated to the computing device. In this
5 example, each of the selectors 1202, 1204 are sliders that can be manipulated with
6 a user input device such as a mouse. By adjusting the cost (or the bandwidth
7 allocation), the user can adjust the allocated bandwidth that they use to transmit
8 their data packets. Accordingly, if a user is in a hurry (e.g. between flights in a
9 busy airport), they could simply adjust one or both of the selectors to
10 automatically select a high level of service that is available. In addition, a data
11 rate display 1206 is provided that displays indicia of a data rate that is currently
12 being provided to the computing device. This gives the user real time feedback so
13 that they can confirm that they are in fact receiving the level of service that they
14 selected and for which they will be charged.

15

16 **Conclusion**

17 The above-described methods and systems provide a mechanism for
18 enhancing wireless functionality in the local area and pushing local area wireless
19 system perform and functionality into the wide area space. High speed wireless
20 Internet access can be provided in public spaces where host organization networks
21 have been deployed. Access can be achieved at speeds up to 100x faster than
22 traditional wireless WAN and 3G solutions. Various embodiments provide an
23 individual-centric approach that enables users to pay for different levels of service,
24 or to have different levels of service provided through arrangements with third
25 party organizations. Enhanced services can be based on pricing and can include

1 access to local network resources, policy-based networking and on-demand
2 security. Aspects of the described embodiments provide for
3 authentication/authorization, negotiation of services with service providers,
4 service enforcement, security and user charging.

5 Although the invention has been described in language specific to structural
6 features and/or methodological steps, it is to be understood that the invention
7 defined in the appended claims is not necessarily limited to the specific features or
8 steps described. Rather, the specific features and steps are disclosed as preferred
9 forms of implementing the claimed invention.

CONTINUED ON PAGE 2